UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

RALF WERNER, *on behalf of himself and all others similarly situated,* *Plaintiff,* **v.** JERICO PICTURES, INC., d/b/a NATIONAL PUBLIC DATA, *Defendant,*	**Case No.:** **COMPLAINT** **CLASS ACTION** **DEMAND FOR A JURY TRIAL**

Plaintiff, Ralf Werner ("Plaintiff"), individually, on behalf of himself and all others similarly situated, brings this action against Defendant JERICO PICTURES, INC. d/b/a NATIONAL PUBLIC DATA, and alleges as follows:

NATURE OF THE ACTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from JERICO PICTURES, INC. d/b/a NATIONAL PUBLIC DATA ("NPD"), arising from its failure to safeguard certain Personally Identifying Information[1] (collectively, "PII") of scores of consumers. Consequently, a broad spectrum of those consumers' PII—including their

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, Plaintiff is not asserting that every example of identifying information was compromised in the Data Breach.

names, email addresses, phone numbers, social security numbers, and mailing addresses—has been compromised.[2]

2. According to its website notice titled, simply, "Security Incident" (NPD's "Notice"), NPD explains that "[t]here appears to have been a data security incident that may have involved some of [the putative class members'] personal information. The incident is believed to have involved a third-party bad actor that was trying to hack into data in late December 2023, with potential leaks of certain data in April 2024 and summer 2024."[3] Upon investigating, NPD determined that "[t]he information that was suspected of being breached contained name, email address, phone number, social security number, and mailing address(es)…" (the "Data Breach").[4]

3. That means that cybercriminals infiltrated NPD's data systems in December of 2023, and had *until the following summer* to exfiltrate the sensitive and confidential PII therein before they escaped unscathed. Six months or more is an eternity for cybercriminals to have unfettered access to NPD's data systems, as evidenced by the scores of consumers whose PII they managed to pilfer.

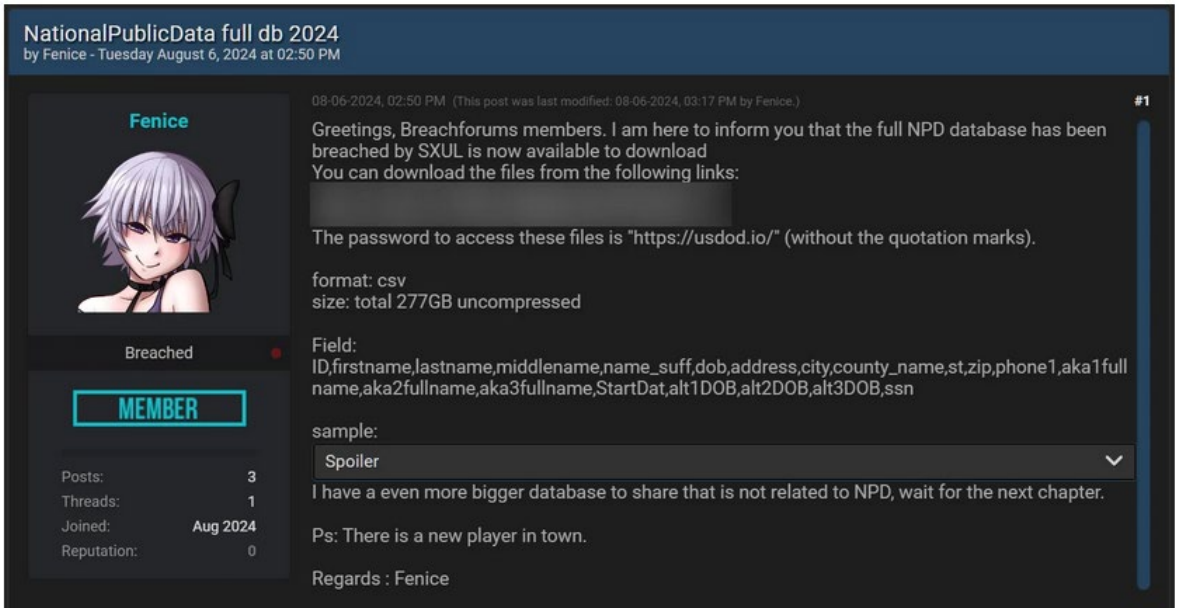
4. According to *Bleeping Computer* and numerous other publications, that dataset originally appeared on the dark web.[5] Evidently, in April, a threat actor known as USDoD claimed to be selling *2.9 billion records* containing PII of consumers from the United States, United Kingdom, and Canada that it

---

[2] *Security Incident*, NAT'L PUB. DATA, *available at* https://nationalpublicdata.com/Breach.html, (last accessed Aug. 15, 2024).
[3] *Ibid.*
[4] *Ibid.*
[5] *See* Lawrence Abrams, *Hackers leak 2.7 billion data records with Social Security numbers*, BLEEPING COMPUTER, *available at* https://www.bleepingcomputer.com/news/security/hackers-leak-27-billion-data-records-with-social-security-numbers/, (Aug. 11, 2024).

lifted from NPD.[6] USDoD claimed that the dataset contained records *for every person* in those three countries, and attempted to sell the data for $3.5 million.[7]

5. Since then, various other threat actors have been leaking data from the NPD dataset. For example, a threat actor named "Fenice" leaked two unencrypted text files totaling 277GB and containing nearly 2.7 billion plaintext records *for free* on the dark web:



[8]

Preliminary investigation by *Bleeping Computer* confirmed that the NPD records leaked by Fenice include names, mailing addresses, and social security numbers, with some records including additional information, like other names associated with those people whose PII was compromised.[9]

6. As will be more fully explained below, Plaintiff and members of the Class have been significantly injured by the Data Breach and have incurred out-of-pocket expenses associated with the reasonable mitigation measures they were forced to employ. Plaintiff and the Class also now forever face an

[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid.*

amplified risk of fraud and identity theft due to their sensitive PII falling into the hands of cybercriminals.

7. On behalf of himself and the Class preliminarily defined below, Plaintiff brings causes of action sounding in negligence, *per se* negligence, invasion of privacy, trespass to chattels, and conversion. Plaintiff seeks damages and injunctive and declaratory relief arising from NPD's failure to adequately protect his highly sensitive PII.

PARTIES

8. Plaintiff Ralf Werner is a natural person and citizen of the State of Tennessee, residing in Antioch, Tennessee, where he intends to remain. Plaintiff received an alert from MyIDCare, a service he pays for, notifying him that his PII, including his phone number and Social Security Number, were compromised in the NPD data breach, and found on the dark web on July 28, 2024 (attached as Exhibit A).

9. Defendant JERICO PICTURES, INC. d/b/a NATIONAL PUBLIC DATA is a Florida Profit Corporation operating under a registered fictitious name which operates as a data aggregator that provides "criminal records, background checks and more"[10], and its principal place of business is located at 1801 NW 126th Way, Coral Springs, Florida 33071. Jerico Pictures, Inc. d/b/a National Public Data's registered agent for service of process in Florida is listed as Salvatore Verini, Jr., 1801 NW 126th Way, Coral Springs, Florida 33071.

JURISDICTION

10. This Court has subject matter jurisdiction over this case based on diversity of citizenship under 28 U.S.C. § 1332 because the amount in

[10] *About Us*, NAT'L PUB. DATA, *available at* https://nationalpublicdata.com/about-us.html, (last accessed Aug. 15, 2024).

controversy exceeds $75,000 and the citizenship of the parties at issue are diverse.

11. This Court also has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because it is brought on behalf of a proposed class with at least 100 members for whom the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest and costs, and Plaintiff and other members of the class are citizens of a State and/or States different from NPD.

12. This Court has general personal jurisdiction over NPD because NPD's principal place of business is in Florida, and it regularly transacts business within the State, such that it is at home within the forum.

VENUE

13. Venue is proper in this Court under 28 U.S.C. §§ 1391(a)(2), (b)(2) & (c)(2) because NPD has its principal place of business in this District and a substantial part of the events giving rise to the claims arise from NPD's business activities in this District.

FACTUAL ALLEGATIONS

A. NPD acquired and aggregated Plaintiff's and the Class Members' PII

14. Plaintiff and the members of the Class are individuals whose sensitive PII was acquired, aggregated and stored in NPD's data systems.

15. NPD acquired and aggregated massive amounts of PII, including, but not limited to, names, email addresses, phone numbers, social security numbers, mailing addresses and aliases.

16. According to NPD, all its "data is updated regularly. [It] guarantee[s] freshness and quality. Search billions of records with instant results, and many searches are no hit/no fee. [Its] services are currently used

by private investigators, consumer public record sites, human resources, staffing agencies and more. Join now and enjoy quality data with low fees."[11]

17. By obtaining, collecting, using, and deriving a financial benefit from those individuals' PII, NPD assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their PII from unauthorized disclosure and misuse.

B. The security of consumers' PII was compromised in the Data Breach

18. Plaintiff's and Class members' PII was acquired, aggregated and stored by NPD.

19. NPD posted a public notice on its website notifying Plaintiff and all Class members that their PII had been compromised during the Data Breach.[12]

20. According to NPD, "[t]here appears to have been a data security incident that may have involved some of [the putative class members'] personal information. The incident is believed to have involved a third-party bad actor that was trying to hack into data in late December 2023, with potential leaks of certain data in April 2024 and summer 2024."[13]

21. NPD further explained that the unknown actor(s) gained access to a panoply of sensitive and confidential PII including "name[s], email address[es], phone number[s], social security number[s], and mailing address(es)…"[14]

[11] *Ibid.*
[12] *See, e.g., Security Incident*, *supra* note 2.
[13] *Ibid.*
[14] *Ibid.*

22. As a result of the Data Breach, the PII for potentially *billions* of innocent consumers was compromised.[15]

23. NPD's Notice did not explain how the Data Breach happened, who perpetrated it, whether a ransom was demanded or paid, or when NPD discovered that their data systems had been infiltrated.

24. Further, upon information and belief, it appears that NPD became aware of the Data Breach on or about April of 2024, yet it neglected to address the issue until the summer, as additional data was compromised up until then.

25. The Data Breach was preventable and a direct result of NPD's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' PII.

C. Data aggregators like NPD are a prime target for cybercriminals

26. On January 29, 2024, Fulton County, Georgia's government systems became the victim of a cyberattack.[16] Likewise, the Kansas court system fell victim to a ransomware attack in October of 2023 that resulted in suspension of its electronic case system for five weeks.[17]

27. The upshot of those two cyberattacks is that "[t]he background screening industry faces a growing threat – cyberattacks targeting court systems and jeopardizing crucial data, halting criminal background check investigations. These attacks disrupt access to vital public records, leaving background checks in limbo and potentially exposing sensitive information."[18]

---

[15] *See* Abrams, *supra*, note 5.
[16] Spells, Alta, *et al.*, *Fulton County government outage: Cyberattack brings down phones, court site and tax systems*, CNN, *available at* https://www.cnn.com/2024/01/30/tech/fulton-county-cyberattack/index.html, (Jan. 30, 2024).
[17] Hollingsworth, Heather, *Kansas officials blame 5-week disruption of court system on 'sophisticated foreign cyberattack'*, ASSOC. PRESS, *available at* https://apnews.com/article/kansas-courts-cyberattack-hack-network-offline-097a11cfa9de552ec5a9ea49b500d3d6, (Nov. 21, 2023).
[18] Kelland, Nick, *Cyberattacks: A Growing Threat to the Background Screening Industry*, INFORMDATA, *available at https://www.informdata.com/blog/cyberattacks-a-growing-threat-to-*

28. Given the increased prevalence of those kinds of breaches, it is incumbent on data aggregators like NPD to institute robust data-security hygiene:

> The cyberattacks on court systems are a wake-up call for the background screening industry. By prioritizing data security and implementing strong cybersecurity measures, CRAs and background screening companies can protect themselves and their clients from the growing threat of cyberattacks. Additionally, advocating for improved cybersecurity measures in court systems is essential to ensure the continued integrity of background checks and protect sensitive personal information.[19]

29. And the PII that NPD failed to protect is particularly valuable, too. The PII stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—including names and social security numbers—is difficult, if not impossible, to change.

30. This data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[20] Likewise, the FBI has warned healthcare organizations that PII data is worth 10 times as much as personal credit card data on the black market.[21]

---

the-background-screening-industry, (Feb. 8, 2024).

[19] *Ibid.*

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[21] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information. *See* Humer, Caroline & Finkle, Jim, *Your medical record is worth more to hackers than your credit card*, REUTERS, (Sep. 24, 2014),

31. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining patient numbers with false provider numbers to file fake claims with insurers.

32. The value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

D. NPD failed to sufficiently protect the PII that it acquired and aggregated

i. NPD failed to adhere to FTC guidelines

33. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[22] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as NPD, should employ to protect against the unlawful exposure of PII.

34. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for businesses.[23] The guidelines explain that businesses should:

---

https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924. Dark web monitoring is a commercially available service which, at a minimum, NPD can and should perform (or hire a third-party expert to perform).

[22] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[23] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016),

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

35. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[24]

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[24] *See Start with Security*, *supra* note 22.

37. NPD's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

ii. NPD failed to adhere to industry standards

38. Numerous industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls, and all data holders are strongly advised to follow these guidelines.[25]

39. Other cybersecurity best practices that are standard in the data security industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and the protection of physical security systems; protecting against any possible communication system; and training staff regarding critical points.

40. Upon information and belief, NPD failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the CIS's Critical Security Controls, which are established frameworks for reasonable cybersecurity readiness.

41. Indeed, InformData recommends the following data security protocols specifically for the background screening industry—NPD's industry:

[25] *CIS Benchmarks FAQ*, CTR. FOR INTERNET SEC., *available at* https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/, (last accessed June 7, 2022).

a. Fortify Your Defenses: Implement robust security protocols, including firewalls, data encryption, and multi-factor authentication (MFA). Regularly update software and conduct vulnerability assessments.

b. Minimize Data Collection and Storage: Only collect and store data necessary for legitimate business purposes. Securely dispose of outdated information.

c. Educate Employees: Train employees on cybersecurity best practices, such as phishing awareness and password security.

d. Stay Informed: Stay current on the latest cyber threats and adapt security measures accordingly.[26]

42. Despite the abundance and availability of information regarding cybersecurity best practices for the background screening industry, NPD failed to adopt sufficient data security processes, a fact highlighted by the fact that it did not detect the Data Breach for at least six months after it happened.

43. NPD failed to adequately train its employees on even the most basic of cybersecurity protocols, which could have prevented the Data Breach.

44. NPD's failure to implement these rudimentary measures made it an easy target for the Data Breach that came to pass.

E. Plaintiff and the Class Members were significantly harmed by the Data Breach

45. As discussed above, PII is among the most sensitive, and personally damaging information.

46. As a result of the Data Breach, Plaintiff now faces, and will continue to face, a heightened risk of identity theft and fraud for the rest of his life.

[26] *Cyberattacks: A Growing Threat to the Background Screening Industry, supra,* note 18.

47. As a long-standing member of the background screening community, NPD knew or should have known the importance of safeguarding the PII that it collected and of the foreseeable consequences of a breach. Despite this knowledge, however, NPD failed to take adequate cyber-security measures to prevent the Data Breach from happening.

48. NPD has not provided any compensation to consumers victimized in the Data Breach and has not offered to provide any assistance or compensation for the costs and burdens—current and future—associated with the identity theft and fraud resulting from the Data Breach.

49. Even if NPD did reimburse Plaintiff for the harm he suffered, it is incorrect to assume that reimbursing a victim of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[27]

50. As a result of NPD's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer significant damages. They have suffered or are at increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise, publication and/or theft of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or

[27] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

fraud, including the purchase of identity theft protection insurance and detection services;

e. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII;

h. The continued risk to their PII, which remains in the possession of NPD and is subject to further breaches so long as NPD fails to undertake appropriate measures to protect the PII in their possession; and

i. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

51. Plaintiff has already incurred harm as a result of the Data Breach.

52. For example, Plaintiff has been forced, and will continue to be forced, to expend time and effort in order to mitigate the harm he has suffered on account of the Data Breach.

53. Plaintiff has expended considerable time and effort attempting to contact NPD and monitoring his identity and credit reports periodically, in addition to gathering documentation.

CLASS ACTION ALLEGATIONS

54. Plaintiff brings this action on behalf of himself and as a class action on behalf of the following proposed class and subclass (collectively, "the Class"):

> (Nationwide Class) All individuals whose PII was compromised in NPD's Data Breach.
>
> (Tennessee Subclass) All citizens of the State of Tennessee whose PII was compromised in NPD's Data Breach.

55. Excluded from the Class are the officers, directors, and legal representatives of NPD and the judges and court personnel in this case and any members of their immediate families.

56. This action is properly maintainable as a class action under Fed. R. Civ. Proc. 23 and the case law thereunder.

57. The Class is so numerous that joinder of all members would be impracticable. Upon information and belief, the Class consists of millions, if not billions of members, spread across numerous states.

58. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether and to what extent NPD had a duty to protect the PII of Plaintiff and the Class;

b. Whether NPD failed to adopt the practices and procedures necessary to adequately safeguard the information compromised in the Data Breach;

c. Whether NPD adequately and accurately informed Class Members that their PII had been compromised;

d. Whether Class Members are entitled to actual damages, statutory damages, and/or punitive damages as a result of NPD's wrongful conduct; and

e. Whether Plaintiff and the Class are entitled to restitution as a result of NPD's wrongful conduct.

59. Plaintiff's claims are typical of those of other Class members because his PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by NPD's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

60. Plaintiff will fairly and adequately represent and protect the interests of the Class in that he has no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

61. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the questions identified in Paragraph 57 above.

62. A class action would provide substantial benefits over other methods for the fair and efficient adjudication of this controversy, as the

pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

63. The litigation of the claims brought herein is manageable. NPD's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

64. Adequate notice can be given to Class members directly using information maintained in NPD's records.

65. This proposed class action does not present any unique management difficulties.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

NEGLIGENCE

66. Plaintiff repeats and incorporates by reference Complaint paragraphs 1-7, & 13-53, *supra*.

67. NPD collected and aggregated Plaintiff's and the Class members' PII.

68. NPD had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if their PII was wrongfully disclosed.

69. NPD had a duty to exercise ordinary and reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, *inter alia*, designing, maintaining and testing NPD's security protocols to ensure that Plaintiff's and Class members' PII in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cyber security measures regarding patient PII.

70. Plaintiff and the Class members were the foreseeable and probable victims of any inadequate security practices and procedures that NPD employed. NPD knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, that it had inadequately trained its employees, and that its security protocols were insufficient to secure the PII of Plaintiff and Class members.

71. NPD's own conduct created a foreseeable risk of harm to Plaintiff and Class members. NPD's misconduct included, but was not limited to, its failure to take the steps to prevent the Data Breach as set forth herein. NPD's misconduct also included its decision to not comply with industry standards for the safekeeping of PII.

72. Plaintiff and the Class members had no ability to protect their PII once NPD collected it.

73. NPD has admitted that Plaintiff's and the Class members' PII was wrongfully disclosed to cybercriminals because of the Data Breach.

74. NPD breached its common law duties to Plaintiff and the Class by failing to exercise ordinary and reasonable care in protecting and safeguarding their PII while it was within NPD's possession or control.

75. NPD unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of its consumers' PII.

76. NPD also unlawfully breached its common law duty to adequately disclose to Plaintiff and Class members the existence and scope of the Data Breach.

77. But for NPD's wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class Members' PII/PHI would not have been compromised.

78. As a result of NPD's negligence, Plaintiff and the Class have suffered and will continue to suffer damages and injury including, but not limited to, out-of-pocket expenses associated with mitigating against the heightened risk of identity theft and fraud caused by the Data Breach; the time and costs associated with remedying identity theft and fraud fairly attributable to the Data Breach; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

79. These harms were directly and proximately caused by the Data Breach.

SECOND CLAIM FOR RELIEF

NEGLIGENCE *Per Se*

80. Plaintiff repeats and incorporates by reference Complaint paragraphs 1-7, & 13-53, *supra*.

81. NPD collected and aggregated Plaintiff's and the Class members' PII.

82. NPD had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if their PII was wrongfully disclosed.

83. NPD had a duty under the FTC Act to, *inter alia*, exercise ordinary and reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, *inter alia*, designing, maintaining and testing NPD's security protocols to ensure that Plaintiff's and Class members' PII in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cyber security measures regarding PII.

84. Plaintiff and the Class members were the foreseeable and probable victims of any inadequate security practices and procedures that NPD employed. NPD knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, that it had inadequately trained its employees, and that its security protocols were insufficient to secure the PII of Plaintiff and Class members.

85. NPD's own conduct created a foreseeable risk of harm to Plaintiff and Class members. NPD's misconduct included, but was not limited to, its failure to take the steps to prevent the Data Breach as set forth herein. NPD's misconduct also included its decision to not comply with the standards imposed by the FTC Act for the safekeeping of patient PII.

86. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as NPD, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of NPD's duty in this regard.

87. NPD further violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry

standards, as described herein. NPD's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class members.

88. Plaintiff and the Class members had no ability to protect their PII once NPD collected it.

89. NPD has admitted that Plaintiff's and the Class members' PII was wrongfully disclosed to cybercriminals because of the Data Breach.

90. NPD breached its duties under the FTC Act to Plaintiff and the Class by failing to exercise ordinary and reasonable care in protecting and safeguarding their PII while it was within NPD's possession or control.

91. NPD also unlawfully breached its duties to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of the PII it collected.

92. NPD also unlawfully breached its duty to adequately disclose to Plaintiff and Class members the existence and scope of the Data Breach.

93. But for NPD's wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class Members' PII would not have been compromised.

94. As a result of NPD's negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer damages and injury including, but not limited to, out-of-pocket expenses associated with mitigating against the heightened risk of identity theft and fraud caused by the Data Breach; the time and costs associated with remedying identity theft and fraud fairly attributable to the Data Breach; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

95. These harms were directly and proximately caused by the Data Breach.

THIRD CLAIM FOR RELIEF

INVASION OF PRIVACY

96. Plaintiff repeats and incorporates by reference Complaint paragraphs 1-7, & 13-53, supra.

97. Plaintiff and Class members took reasonable and appropriate steps to keep their PII confidential from the public.

98. Plaintiff's and Class members' efforts to safeguard their own PII were successful, as their PII was not known to the general public prior to the Data Breach.

99. Plaintiff and Class members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

100. NPD owed a duty to those individuals whose PII it collected, including Plaintiff and Class members, to keep their PII confidential.

101. The unauthorized release of PII, especially PHI, is highly offensive to a reasonable person.

102. Plaintiff's and Class members' PII is not of legitimate concern to the public.

103. NPD publicized Plaintiff's and Class members' PII, by communicating it to cyber criminals who had no legitimate interest in this PII and who had the express purpose of monetizing that information by injecting it into the illicit stream of commerce flowing through the dark web.

104. Indeed, not only is Plaintiff's and Class members' PII traveling the dark web, but it is being used to commit fraud; it is being disseminated

amongst, *inter alia*, merchants, creditors, health care providers and governmental agencies.

105. It is therefore substantially certain that the Plaintiff's and the Class members' PII is rapidly becoming public knowledge – among the cybercriminal community writ large – due to the nature of the Data Breach that procured it, and the identity theft that it is designed for.

106. Unless and until enjoined, and restrained by order of this Court, NPD's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that NPD's inadequate data security measures will likely result in additional data breaches. Plaintiff and Class members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiff's and Class members' privacy by NPD.

FOURTH CLAIM FOR RELIEF

TRESPASS TO CHATTELS

107. Plaintiff repeats and incorporates by reference Complaint paragraphs 1-7, & 13-53, *supra*.

108. NPD collected and aggregated Plaintiff's and the Class members' PII.

109. NPD intentionally dispossessed the Plaintiff and the putative members of the Class of their PII and/or used or intermeddled with the Plaintiff and the putative members of the Class's possession of their PII, when it allowed cybercriminals to access it.

110. As explained at length above, Plaintiff and the Class members were damaged thereby.

FIFTH CLAIM FOR RELIEF

CONVERSION

111. Plaintiff repeats and incorporates by reference Complaint paragraphs 1-7, & 13-53, *supra*.

112. At all times relevant hereto, Plaintiff and Class Members had ownership rights to their PII.

113. NPD engaged in the wrongful act of disposing of the PII by giving cyber criminals access to it.

114. As explained at length above, Plaintiff and the Class were damaged thereby.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, on behalf of himself, and all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and his counsel as Class counsel;

B. A mandatory injunction directing NPD to safeguard the PII of Plaintiff and the Class hereinafter adequately by implementing improved security procedures and measures;

C. A mandatory injunction requiring that NPD provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. An award of compensatory, restitutionary, punitive, exemplary, and statutory damages, as permitted by law.

E. An award of attorneys' fees and costs;

F. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: August 20, 2024

Respectfully submitted,

/s/ Tricia R. Herzfeld

Tricia R. Herzfeld (FL Bar #0529680)
Joe P. Leniski, Jr.*
HERZFELD, SUETHOLZ, GASTEL, LENISKI & WALL PLLC
223 Rosa L. Parks Avenue
Suite 300
Nashville, Tennessee 37203
Telephone: (615) 800-6225
Email: tricia@hsglawgroup.com
joey@hsglawgroup.com

Peter J. Jannace*
HERZFELD, SUETHOLZ, GASTEL, LENISKI & WALL PLLC
515 Park Avenue
Louisville, Kentucky 40208
Telephone: (502) 636-4333
Email: peter@hsglawgroup.com
**PHV Application Pending*
Attorneys for Plaintiff